ECC Certificate Addendum to the Comodo EV Certification Practice Statement v.1.03

Comodo CA, Ltd.
ECC Certificate Addendum to Comodo EV CPS v. 1.03
6 March 2008

3rd Floor, Office Village, Exchange Quay, Trafford Road
Salford, Manchester, M5 3EQ, United Kingdom
www.comodogroup.com

Comodo CA Ltd. (“Comodo”) has recently generated two ECC root certificates. The purpose of this Addendum to the Comodo Certification Practice Statement (“ACPS”) is to amend version 1.03 of the EV Comodo Certification Practice Statement (“CPS”) to include the Comodo’s ECC root certificates in Comodo’s CPS. All provisions of the CPS not specifically amended or added herein remain in full force and effect and where applicable shall apply to the new product offerings. Amended portions in this ACPS are included within brackets. Nothing in the CPS shall be deemed omitted, deleted or amended unless expressly stated in this ACPS or identified in brackets below. Information not located in brackets is to be included in addition to all information in the CPS. Headings from the CPS are included to identify the location of the Amended information, and are not intended to be duplicative.

Acronyms / Terms Used in the ECC Certificate Addendum to Comodo EV CPS:

RSA An asymmetric encryption algorithm suitable for digital signatures.

ECC Elliptic Curve Cryptography – A more modern family of asymmetric encryption algorithms of which ECDSA is suitable for digital signatures.

1 General

. . . .

1.8 Comodo PKI Hierarchy

Comodo uses the COMODO ECC Certification Authority, COMODO Certification Authority, UTN-USERFIRST-Hardware, UTN – DATACorp SGC, and AddTrust External CA Root for its Root CA Certificates for EV Certificates. This allows Comodo to issue highly trusted EV Certificates by inheriting the trust level associated with the Comodo root certificates (named “COMODO ECC Certificate Authority” and “COMODO Certificate Authority”), UTN root certificates (named “UTN-USERFIRST-Hardware” and “UTN – DATACorp SGC"), and the AddTrust root certificate (named “AddTrust External CA Root”). The ability to issue trusted certificates from these different roots provides Comodo with additional flexibility and trust. The following high-level representation of the Comodo PKI is used to illustrate the hierarchy utilized.

1.8.1 EV Certificates

Comodo issues EV certificates from two different root CAs.

Certificates issued from the COMODO ECC Certification Authority are visible on Browsers or platforms that Trust that root as follows:

COMODO ECC Certification Authority (serial number = 1f 47 af aa 62 00 70 50 54 4c 01 93 9b 63 99 2a, expiry = 18 January 2038 23:59:59)

↳ COMODO EV SSL ECC CA (serial number = TBA, expiry = 31 December 2019 23:59:59)

↳ End Entity SSL (*serial number = x, expiry = 12 to 27 months from issuance*)

Certificates issued from the COMODO Certification Authority are:-
Visible on Browsers on platforms that Trust the “COMODO Certification Authority” root as follows:

COMODO Certification Authority (serial number = 4e 81 2d 8a 82 65 e0 0b 02 ee 3e 35 02 46 e5 3d, expiry = 31 December 2029 23:59:59)

↳ COMODO EV SSL CA (serial number = 21 d9 5f 9e a9 bf ee 5d e9 d2 7c e4 0a 4e 21 0c, expiry = 31 December 2019 23:59:59)

↳ End Entity SSL (*serial number = x, expiry = 12 to 27 months from issuance*)

Cross signed and therefore visible on other IE compatible browsers as follows:

UTN-USERFIRST-Hardware (*serial number = 44 be 0c 8b 50 00 24 b4 11 d3 36 2a fe 65 0a fd, expiry = 09 July 2019 19:19:22*)

↳ COMODO Certification Authority (serial number = 50 00 13 44 9f 5b 4e ae c6 3b de a3 9c 5c 33
26, expiry = 30 May 2020 10:48:38)

↳ COMODO EV SSL CA (serial number = 21 d9 5f 9e a9 bf ee 5d e9 d2 7c e4 0a 4e 21 0c, expiry = 31 December 2019 23:59:59)

↳ End Entity SSL (*serial number = x, expiry = 12 to 27 months from issuance*)

Cross signed and therefore visible on Netscape compatible browsers as follows:

AddTrust External CA Root (*serial number = 01, expiry = 30/05/2020 10:48:38*)

↳ UTN-USERFirst-Hardware (serial number = 48 4b ac f1 aa c7 d7 13 43 d1 a2 74 35 49 97 25, expiry = 30 May 2020 11:48:38)

↳ COMODO Certification Authority (serial number = 50 00 13 44 9f 5b 4e ae c6 3b de a3 9c 5c 33 26, expiry = 30 May 2020 10:48:38)

↳ COMODO EV Certification Authority (serial number = 21 d9 5f 9e a9 bf ee 5d e9 d2 7c e4 0a 4e 21 0c, expiry = 31 December 2019 23:59:59)

↳ End Entity SSL (*serial number = x, expiry = 12 to 27 months from issuance*)

1.8.2 EV SGC

Visible on Browsers on platforms that Trust the “COMODO Certification Authority” root as follows:

COMODO Certification Authority (serial number = 4e 81 2d 8a 82 65 e0 0b 02 ee 3e 35 02 46 e5 3d, expiry = 31 December 2029 23:59:59)

↳ COMODO EV SGC CA (serial number = 13 62 e8 eb 54 1a 10 8c b8 a8 0e e5 9f b1 d4 51, expiry = 31 December 2019 23:59:59)

↳ End Entity SSL (*serial number = x, expiry = 12 to 27 months from issuance*)

Cross signed and therefore visible on other IE compatible browsers as follows:

UTN - DATACorp SGC (*serial number = 44 be 0c 8b 50 00 21 b4 11 d3 2a 68 06 a9 ad 69, expiry = 24 June 2019 19:06:30*)

↳ COMODO Certification Authority (serial number = 7e 9a a1 af 78 3c 42 2e 72 30 ce ee e3 c2 7f a6, expiry = 30 May 2020 10:48:38)

↳ COMODO EV SGC CA (serial number = 13 62 e8 eb 54 1a 10 8c b8 a8 0e e5 9f b1 d4 51, expiry = 31 December 2019 23:59:59)

↳ End Entity SSL (*serial number = x, expiry = 12 to 27 months from issuance*)

Cross signed and therefore visible on Netscape compatible browsers as follows:

AddTrust External CA Root (*serial number = 01, expiry = 30/05/2020 10:48:38*)

↳ UTN - DATACorp SGC (serial number = 53 7b 76 56 4f 29 7f 14 dc 69 43 e9 22 ad 2c 79, expiry = 30 May 2020 10:48:38)

↳ COMODO Certification Authority (serial number = 7e 9a a1 af 78 3c 42 2e 72 30 ce ee e3 c2 7f a6, expiry = 30 May 2020 10:48:38)

↳ COMODO EV SGC CA (serial number = 13 62 e8 eb 54 1a 10 8c b8 a8 0e e5 9f b1 d4 51, expiry = 31 December 2019 23:59:59)

↳ End Entity SSL (*serial number = x, expiry = 12 to 27 months from issuance*)

. . . .

2.1.1 Root CA Signing Key Protection & Recovery

The Comodo CA certificates for signing EV Certificates are shown below in Table 2.1.1. Protection of Comodo Root signing key pairs is ensured with the use of IBM 4578 cryptographic coprocessor devices or Utimaco SafeGuard CryptoServer devices certified to FIPS 140 (-1 or -2) Level 4, for key generation, storage, and use. Comodo Root signing key pairs are RSA 2048 bit or ECC 384 bit and were generated within the above mentioned devices respectively.

. . . .

1001	COMODO ECC Certificate Authority	Root CA for COMODO Certificates including EV	19 January 2038	ECC384
1002	COMODO EV SSL ECC CA	Intermediate CA for EV certificates	31 December 2019	ECC384

Comodo protects its Comodo, UTN, and AddTrust CA Root key pairs in accordance with its AICPA/CICA WebTrust program compliant infrastructure and EV CPS. Details of Comodo's WebTrust compliance are available at Comodo's official website (www.comodogroup.com).

2.1.2 CA Root Signing Key Generation Process

Comodo securely generates and protects its own private key(s) using a trustworthy system (IBM 4758 accredited to FIPS PUB 140-1 level 4 or Utimaco SafeGuard CryptoServer accredited to FIPS PUB 140-2 level 4), and takes necessary precautions to prevent the compromise or unauthorized usage of it.

The Comodo CA Root keys were generated in accordance with the guidelines detailed in the Root Key Generation Ceremony Reference. The activities undergone and the personnel involved in the Root Key Generation Ceremony are recorded for audit purposes. Subsequent Root Key Generation Ceremonies are to follow the documented reference guide also.

. . . .

2.12.5 CA Root Signing Key Generation Process

. . . .

The specific Comodo EV Certificate profile is as per the table below:

Comodo EV Secure Server Certificates		
Signature Algorithm	Sha1	
Issuer	CN	COMODO EV Certification Authority
	O	COMODO CA Limited
	L	Salford
	S	Greater Manchester
	C	GB
Validity	12 to 27 months	

Subject	CN	Domain name	
	OU	Comodo EV SSL / Comodo EV SGC SSL	
	OU (0 or 1 of)	*Hosted by [Web Host Reseller Subscriber Name]* *Issued through [EPKI Manager Subscriber Name]* *Provided by [Powered SSL Subscriber Name]*	
	O	Organization	
	OU	Organization Unit	
	L	Locality (City)	
	STREET	Street	
	S	State	
	PostalCode	Zip or Postal Code	
	C	Country	
	jurisdictionOfIncorporationLocalityName		Locality
	jurisdictionOfIncorporationStateOrProvinceName		State
	jurisdictionOfIncorporationCountryName		Country
	serialNumber	Registration Number	
Authority Key Identifier	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.comodoca.com		
Key Usage (NonCritical)	Digital Signature, Key Encipherment(A0)		
Extended Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2) and for SGC certificates only: Microsoft Server Gated Crypto (1.3.6.1.4.1.311.10.3.3) Netscape Server Gated Crypto (2.16.840.1.113730.4.1)		
Netscape Certificate Type	SSL Client Authentication, SSL Server Authentication(c0)		
Basic Constraint	Subject Type = End Entity Path Length Constraint = None		
Certificate Policies	1] Certificate Policy: PolicyIdentifier = 1.3.6.1.4.1.6449.1.2.1.5.1 [1,1]Policy Qualifier Info: Policy Qualifier Id = CPS Qualifier: http://www.comodogroup.com/repository/EV_CPS.pdf		
CRL Distribution Policies	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.comodoca.com/COMODOEVSSLCA.crl (or for SGC certificates URL= http://crl.comodoca.com/COMODOEVSGCCA.crl) (or for EV certificates issued from the ECC root URL=http://crl.comodoca.com/COMODOEVSSLECCCA.crl)		
Thumbprint Algorithm	*SHA1*		
Thumbprint			

. . . .

Document Control

This document is the ECC Certificate Addendum to Comodo CPS Version 1.03, created on 6 March 2008 and signed off by the Comodo Certificate Policy Authority.

Comodo CA Limited
3rd Floor, Office Village, Exchange Quay, Trafford Road,
Salford, Manchester, M5 3EQ, United Kingdom
URL: http://www.comodogroup.com

Email: legal@comodogroup.com

Tel: +44 (0) 161 874 7070
Fax: +44 (0) 161 877 1767